NOTE: [More related information is available here](#).

NORTHERN ILLINOIS UNIVERSITY

THE SOCIAL ORGANIZATION OF THE COMPUTER UNDERGROUND

A THESIS SUBMITTED
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE
MASTER OF ARTS

DEPARTMENT OF SOCIOLOGY

BY

GORDON R. MEYER

%CompuServe: 72307,1502%
%GEnie: GRMEYER%

DEKALB, ILLINOIS
AUGUST 1989

ABSTRACT

Name: Gordon R. Meyer   Department: Sociology

Title: The Social Organization of the Computer Underground
Major: Criminology   Degree: M.A.

NORTHERN ILLINOIS UNIVERSITY

ABSTRACT

This paper examines the social organization of the

"computer underground" (CU). The CU is composed of

actors in three roles, "computer hackers," "phone

phreaks," and "software pirates." These roles have

frequently been ignored or confused in media and other

accounts of CU activity. By utilizing a data set culled

from CU channels of communication this paper provides

an ethnographic account of computer underground

organization. It is concluded that despite the

widespread social network of the computer underground,

it is organized primarily on the level of colleagues,

with only small groups approaching peer relationships.

ACKNOWLEDGMENTS

Form SF298 Citation Data

Report Date *("DD MON YYYY")* 01081989	Report Type N/A	Dates Covered (from... to) *("DD MON YYYY")*

Title and Subtitle The Social Organization of the Computer Underground		Contract or Grant Number
		Program Element Number
Authors		Project Number
		Task Number
		Work Unit Number
Performing Organization Name(s) and Address(es) Department of Sociology Northern Illinois University		Performing Organization Number(s)
Sponsoring/Monitoring Agency Name(s) and Address(es)		Monitoring Agency Acronym
		Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited		
Supplementary Notes		
Abstract		
Subject Terms "IATAC COLLECTION"		
Document Classification unclassified		Classification of SF298 unclassified
Classification of Abstract unclassified		Limitation of Abstract unlimited
Number of Pages 57		

REPORT DOCUMENTATION PAGE

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	8/1/89	Report

4. TITLE AND SUBTITLE
The Social Organization of the Computer Underground

5. FUNDING NUMBERS

6. AUTHOR(S)
Gordon Meyer

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
Information Assurance Technology Analysis
Center
3190 Fairview Park Drive
Falls Church VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE

A

13. ABSTRACT *(Maximum 200 Words)*

This paper examines the social organization of the "computer underground" (CU). The CU is composed of actors in three roles, "computer hackers," "phonephreaks," and "software pirates." These roles have frequently been ignored or confused in media and other accounts of CU activity. By utilizing a data set culled from CU channels of communication this paper provides an ethnographic account of computer underground organization. It is concluded that despite the widespread social network of the computer underground, it is organized primarily on the level of colleagues, with only small groups approaching peer relationships.

14. SUBJECT TERMS
HACK, Computer Underground

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	UNCLASSIFIED	UNCLASSIFIED	None

```
                    FOR CRITIQUE, ADVICE, AND COMMENTS:

                            DR. JAMES L. MASSEY
                              DR. JIM THOMAS
                          DR. DAVID F. LUCKENBILL

                      FOR SUPPORT AND ENCOURAGEMENT:
                                GALE GREINKE

                            SPECIAL THANKS TO:

                       D.C., T.M., T.K., K.L., D.P.,
                            M.H., AND G.Z.


                        THIS WORK IS DEDICATED TO:
                             GEORGE HAYDUKE
                                  AND
                             BARRY FREED
```

TABLE OF CONTENTS

Introduction

        The proliferation of home computers has been

accompanied by a corresponding social problem involving

the activities of so-called "computer hackers."

"Hackers" are computer aficionados who "break in" to

corporate and government computer systems using their
home computer and a telephone modem. The prevalence of
the problem has been dramatized by the media and
enforcement agents, and evidenced by the rise of
specialized private security firms to confront the
"hackers." But despite this flurry of attention,
little research has examined the social world of the
"computer hacker." Our current knowledge in this regard
derives from hackers who have been caught, from
enforcement agents, and from computer security
specialists. The everyday world and activities of the
"computer hacker" remain largely unknown.

This study examines the way actors in the
"computer underground" (CU) organize to perform their
acts. The computer underground, as it is called by
those who participate in it, is composed of actors
adhering to one of three roles: "hackers," "phreakers,"
or "pirates." To further understanding this growing
"social problem," this project will isolate and clarify
these roles, and examine how each contributes to the
culture as a whole. By doing so the sociological
question of how the "underground" is organized will be
answered, rather than the technical question of how CU
participants perform their acts.

Best and Luckenbill (1982) describe three basic
approaches to the study of "deviant" groups. The first
approach is from a social psychological level, where
analysis focuses on the needs, motives, and individual
characteristics of the actors involved. Secondly,
deviant groups can be studied at a socio-structural
level. Here the emphasis is on the distribution and
consequences of deviance within the society as a whole.
The third approach, the one adopted by this work, forms
a middle ground between the former two by addressing

the social organization of deviant groups.   Focusing
upon neither the individual nor societal structures
entirely, social organization refers to the network of
social relations between individuals involved in a
common activity (pp. 13-14). Assessing the degree and
manner in which the underground is organized provides
the opportunity to also examine the culture, roles, and
channels of communication used by the computer
underground. The focus here is on the day to day
experience of persons whose activities have been
criminalized over the past several years.

     Hackers, and the "danger" that they present in our
computer dependent society, have often received
attention from the legal community and the media. Since
1980, every state and the federal government has
criminalized "theft by browsing" of computerized
information (Hollinger and Lanza-Kaduce, 1988, pp.101-
102). In the media, hackers have been portrayed as
maladjusted losers, forming "high-tech street gangs"
(Chicago Tribune, 1989) that are dangerous to society.
My research will show that the computer underground
consists of a more sophisticated level of social
organization than has been generally recognized. The
very fact that CU participants are to some extent
"networked" has implications for social control
policies that may have been implemented based on an in-
complete understanding of the activity. This project
not only offers sociological insight into the organ-
ization of deviant associations, but may be helpful to
policy makers as well.

     I begin with a discussion of the definitional
problems that inhibit the sociological analysis of the
computer underground. The emergence of the computer
underground is a recent phenomenon, and the lack of

empirical research on the topic has created an area
where few "standard" definitions and categories exist.
This work will show that terms such as "hacker,"
"phreaker," and "pirate" have different meanings for
those who have written about the computer underground
and those who participate in it. This work bridges
these inconsistencies by providing definitions that
focus on the intentions and goals of the participants,
rather than the legality or morality of their actions.

Following the definition of CU activities is a
discussion of the structure of the underground.
Utilizing a typology for understanding the social
organization of deviant associations, developed by Best
and Luckenbill (1982), the organization of the
computer underground is examined in depth.

The analysis begins by examining the structure of
mutual association. This provides insight into how CU
activity is organized, the ways in which information is
obtained and disseminated, and explores the subcultural
facets of the computer underground. More importantly,
it clearly illustrates that the computer underground is
primarily a social network of individuals that perform
their acts separately, yet support each other by
sharing information and other resources.

After describing mutual association within the
underground community, evidence of mutual participation
is presented. Although the CU is a social network, the
ties developed at the social level encourage the
formation of small "work groups." At this level, some
members of the CU work in cooperation to perform their
acts. The organization and purposes of these groups are
examined, as well as their relationship to the CU as a
whole. However, because only limited numbers of
individuals join these short-lived associations, it is

concluded that the CU is organized as colleagues. Those
who do join "work groups" display the characteristics
of peers, but most CU activity takes place at a fairly
low level of sophistication.

Methodology

Adopting an ethnographic approach, data have been
gathered by participating in, monitoring, and cata-
loging channels of communication used by active members
of the computer underground. These channels, which will
be examined in detail later, include electronic
bulletin board systems (BBS), voice mail boxes,
bridges, loops, e-mail, and telephone conversations.
These sources provide a window through which to observe
interactions, language, and cultural meanings without
intruding upon the situation or violating the privacy
of the participants. Because these communication
centers are the "back stage" area of the computer
underground, they provided insight into organizational
(and other) issues that CU participants face, and the
methods they use to resolve them.

As with any ethnographic research, steps have been
taken to protect the identity of informants. The
culture of the computer underground aids the researcher
in this task since phreakers, hackers, and pirates
regularly adopt pseudonyms to mask their identity.
However to further ensure confidentiality, all of the
pseudonyms cited in this research have been changed by
the author. Additionally, any information that is
potentially incriminating has been removed or altered.

The data set used for this study consists
primarily of messages, or "logs," which are the primary
form of communication between users. These logs were
"captured" (recorded using the computer to save the
messages) from several hundred computer bulletin

boards1 located across the United States. The bulk of

the data were gathered over a seventeen month period

(12/87 to 4/89) and will reflect the characteristics of

the computer underground during that time span.

However, some data, provided to the researcher by

cooperative subjects, dates as far back as 1984.

The logged data were supplemented by referring to

several CU "publications." The members of the computer

underground produce and distribute several technical

and tutorial newsletters and "journals." Since these

"publications" are not widely available outside of CU

circles I have given a brief description of each below.

Legion of Doom/Hackers Technical Journal. This

_____

1 Computer Bulletin Boards (BBS) are personal
computers that have been equipped with a telephone
modem and special software. Users can connect with a
BBS by dialing, with their own computer and modem, the
phone number to which the BBS is connected. After
"logging in" by supplying a valid user name and pass-
word, the user can leave messages to other users of the
system. These messages are not private and anyone
calling the BBS can freely read and respond to them.
publication is written and distributed by a group known
as "The Legion of Doom/Legion of Hackers" (LoD/H). It
is available in electronic format (a computer text
file) and contains highly technical information on
computer operating systems. As of this writing, three
issues have been published.

PHRACK Inc.: Phrack Inc is a newsletter that

contains various articles, written by different

authors, and "published" under one banner. Phrack

Inc's first issue was released in 1985, making it the

oldest of the electronically distributed underground

publications. CU participants are invited to submit

articles to the editors, who release a new issue when a

sufficient number (about nine) of acceptable pieces

have been gathered. Phrack also features a lengthy

"World News" with stories about hackers who have been

apprehended and interviews with various members of the

underground. As of this writing twenty-seven issues of

Phrack, have been published.

Phreakers/Hackers Underground Network (P/Hun):
Like Phrack, P/Hun collects articles from various
authors and releases them as one issue. Three issues
have been published to date.

Activist Times, Incorporated (ATI): Unlike the
other electronically distributed publications, ATI does
not limit itself to strictly computer/telephone news.
Articles normally include commentary on world and
government events, and other "general interest" topics.
ATI issues are generally small and consist of articles
written by a core group of four to seven people.
Unlike the publications discussed thus far, ATI is
available in printed "hard copy" form by sending
postage reimbursement to the editor. ATI is currently
on their 38th issue.

2600 Magazine: Published in a traditional
(printed) magazine format, 2600 (named for the
frequency tone used to make free long distance phone
calls) is arguably an "underground" publication as it
is available on some newsstands and at some libraries.
Begun in 1987 as a monthly magazine, it is now
published quarterly. Subscription rates are $25.00 a
year with a complete back-issue selection available.
The magazine specializes in publishing technical
information on telephone switching systems, satellite
descrambling codes, and news about the computer
underground.

TAP/YIPL: First established in 1972 as YIPL (Youth
International Party Line), this publication soon
changed its name to TAP (Technical Assistance Party).
Co-founded by Abbie Hoffman, it is generally recognized
as the grandfather of computer underground
publications. Publication of the 2-4 page newsletter

has been very sporadic over the years, and currently
two different versions of TAP, each published in
different areas of the country, are in circulation.

Utilizing a data set that consists of current
message logs, old messages logs, and various CU
publications yields a reasonably rich collection from
which to draw the analysis. Examination of the older
logs and publications shows that while the actors have
changed over the years, cultural norms and
characteristics have remained consistent over time.

What is the Computer Underground?

Defining the "computer underground" can be
difficult. The sociologist soon finds that there are
several competing definitions of computer underground
activity. Those who have written on the subject, the
media, criminologists, computer programmers, social
control agents, and CU participants themselves, have
adopted definitions consistent with their own social
positions and perspectives. Not surprisingly, these
definitions rarely correspond. Therefore, before
discussing the organization of the computer
underground, it is necessary to discuss and compare the
various definitions. This will illustrate the range of
beliefs about CU activity, and provide a springboard
for the discussion of types of roles and activities
found in the underground.

We begin with a discussion of the media image of
computer hackers. The media's concept of "hackers" is
important because the criminalization of the activity
has largely occurred as the result of media drama-
tization of the "problem" (Hollinger and Lanza-Kaduce,
1988). In fact, it was a collection of newspaper and
film clips that was presented to the United States
Congress during legislative debates as evidence of the

computer hacking problem (Hollinger and Lanza-Kaduce, 1988, p.107). Unfortunately, the media assessment of the computer underground displays a naive understanding of CU activity.

The media generally makes little distinction between different types of CU activity. Most any computer-related crime activity can be attributed to "hackers." Everything from embezzlement to computer viruses have, at one time or another, been attributed to them. Additionally, hackers are often described as being sociopathic or malicious, creating a media image of the computer underground that may exaggerate their propensity for doing damage.

The labeling of hackers as being "evil" is well illustrated by two recent media examples. The first is from Eddie Schwartz, a WGN-Radio talk show host. Here Schwartz is addressing "Anna," a self-identified hacker that has phoned into the show:

> You know what Anna, you know what disturbs
> me? You don't sound like a stupid person but
> you represent a . . . a . . . a . . . lack of
> morality that disturbs me greatly. You really
> do. I think you represent a certain way of
> thinking that is morally bankrupt. And I'm
> not trying to offend you, but I . . . I'm
> offended by you! (WGN Radio, 1988)

Just two months later, NBC-TV's "Hour Magazine" featured a segment on "computer crime." In this example, Jay Bloombecker, director of the National Center for Computer Crime Data, discusses the "hacker problem" with the host of the show, Gary Collins.

> Collins: . . . are they %hackers% malicious
> in intent, or are they simply out to prove,
> ah, a certain machismo amongst their peers?
>
> Bloombecker: I think so. I've talked about
> "modem macho" as one explanation for what's
> being done. And a lot of the cases seem to
> involve %proving% %sic% that he . . . can do
> something really spiffy with computers. But,
> some of the cases are so evil, like causing
> so many computers to break, they can't look
> at that as just trying to prove that you're
> better than other people.

GC: So that's just some of it, some kind of
"bet" against the computer industry, or
against the company.

JB: No, I think it's more than just
rottenness. And like someone who uses
graffiti doesn't care too much whose building
it is, they just want to be destructive.

GC: You're talking about a sociopath in
control of a computer!

JB: Ah, lots of computers, because there's
thousands, or tens of thousands %of hackers%
(NBC-TV, 1988).

The media image of computer hackers, and thus all

members of the computer underground, is burdened with

value-laden assumptions about their psychological

makeup, and focuses almost entirely upon the morality

of their actions. Additionally, since media stories

are taken from the accounts of police blotters,

security personnel, and hackers who have been caught,

each of whom have different perspectives and

definitions of their own, the media definition, if not

inherently biased, is at best inconsistent.

Criminologists, by way of contrast, have done

little to define the computer underground from a

sociological perspective. Those criminological

definitions that do exist are less judgmental than the

media image, but no more precise. Labels of

"electronic trespassers" (Parker, 1983), and

"electronic vandals" (Bequai, 1987) have both been

applied to hackers. Both terms, while acknowledging

that "hacking" is deviant, shy away from labeling it as

"criminal" or sociopathic behavior. Yet despite this

seemingly non-judgmental approach to the computer

underground, both Parker and Bequai have testified

before Congress, on behalf of the computer security in-

dustry, on the "danger" of computer hackers.

Unfortunately, their "expert" testimony was largely

based on information culled from newspaper stories, the
objectiveness of which has been seriously questioned
(Hollinger and Lanza-Kaduce 1988 p.105).

Computer security specialists, on the other hand,
are often quick to identify CU participants as part of
the criminal element. Correspondingly, some reject the
notion that there are different roles and motivations
among computer underground participants and thereby
refuse to define just what it is that a "hacker" or
"phreaker" does. John Maxfield, a "hacker expert,"
suggests that differentiating between "hackers" and
"phone phreaks" is a moot point, preferring instead
that they all just be called "criminals" (WGN-Radio.
Sept 28, 1988).

The reluctance or inability to differentiate
between roles and activities in the computer
underground, as exhibited in the media and computer
security firms, creates an ambiguous definition of
"hacker" that possesses two extremes: the modern-day
bank robber at one end, the trespassing teenager at the
other. Thus, most any criminal or mischievous act that
involves computers can be attributed to "hackers,"2
regardless of the nature of the crime.

Further compounding the inconsistent use of
"hacker" is the evolution of meaning that the word has
undergone.   "Hacker" was first applied to computer
related activities when it was used by programmers in
the late 1950's. At that time it referred to the
pioneering researchers, such as those at M.I.T., who

----

2 During the WGN-Radio show on computer crime one
caller, who was experiencing a malfunctioning phone
that would "chirp" occasionally while hung up, believed
that "computer hackers" were responsible for the
problem. The panel assured her that it was unrelated
to CU activity.

----

were constantly adjusting and experimenting with the

new technology (Levy, 1984. p.7). A "hacker" in this

context refers to an unorthodox, yet talented,

professional programmer. This use of the term still

exits today, though it is largely limited to

professional computing circles.

      Another definition of "hacker" refers to one who

obtains unauthorized, if not illegal, access to

computer systems and networks. This definition was

popularized by the movie War Games and, generally

speaking, is the one used by the media.3 It is also the

definition favored by the computer underground.

      Both the members of the computer underground and

computer programmers claim ownership of "hacker," and

each defend the "proper" use of term. The computer

professionals maintain that using "hackers" (or

"hacking") to refer to any illegal or illicit activity

is a corruption of the "true" meaning of the word. Bob

Bickford, a professional programmer who has organized

several programmer conferences, explains:

_____

     3 This is not always true of course. The AP
Stylebook has yet to specify how "hacker" should be
used. A recent Associated Press story featured a
computer professional explaining that a "real hacker"
would never do anything illegal. Yet just a few weeks
later Associated Press distributed stories proclaiming
that West German "hackers" had broken into US Defense
Department computer systems.
_____

     At the most recent conference %called
     "Hackers 4.0"% we had 200 of the most
     brilliant computer professionals in the world
     together for one weekend; this crowd included
     several PhD's, several presidents of
     companies (including large companies, such as
     Pixar), and various artists, writers,
     engineers, and programmers. These people all
     consider themselves Hackers: all derive great
     joy from their work, from finding ways around
     problems and limits, from creating rather
     than destroying. It would be a great
     disservice to these people, and the thousands
     of professionals like them, to let some
     pathetic teenaged criminals destroy the one
     word which captures their style of
     interaction with the universe: Hackers
     (Bickford, 1988).

     Participants in the computer underground also

object to the "misuse" of the term. Their objection

centers around the indiscriminate use of the word to

refer to computer related crime in general and not,

specifically, the activities of the computer

underground:

> Whenever the slightest little thing happens
> involving computer security, or the breach
> thereof, the media goes fucking bat shit and
> points all their fingers at us 'nasty
> hackers.' They're so damned ignorant it's
> sick (EN, message log, 1988).

> . . . whenever the media happens upon
> anything that involves malicious computer use
> it's the "HACKERS." The word is a catch
> phrase it makes mom drop the dishes and watch
> the TV. They use the word because not only
> they don't really know the meaning but they
> have lack of a word to describe the
> perpetrator. That's why hacker has such a
> bad name, its always associated with evil
> things and such (PA, message log, 1988).

> I never seen a phreaker called a phreaker
> when caught and he's printed in the
> newspaper. You always see them "Hacker caught
> in telephone fraud." "Hacker defrauds old
> man with phone calling card." What someone
> should do is tell the fucken (sic) media to
> get it straight (TP2, message log, 1988).

Obviously the CU and computer professional

definitions of "hacker" refer to different social

groups. As Best and Luckenbill (1982, p. 39) observe:

"Every social group modifies the basic language to fit

its own circumstance, creating new words or using

ordinary words in special ways." Which definition, if

either, will come into widespread use remains to be

seen. However, since computer break-ins are likely to

receive more media attention than clever feats of

programming, the CU definition is likely to dominate

simply by being used more often.4 But as long as the

two definitions do exist there will be confusion unless

writers and researchers adequately specify the group

under discussion. For this reason, I suggest that

sociologists, and criminologists in particular, adopt

the "underground" definition for consistency and
_____

    4 Another factor may be the adoption of a close
proximity to the underground definition being included
in the 1986 edition of Webster's New World dictionary:
    hack.er n. 1. a person who hacks 2. an unskilled
golfer, tennis player, etc. 3. a talented amateur user
of computers, specif. one who attempts to gain
unauthorized access to files.

_____

accuracy when speaking of the actions of CU

participants.

    While it is recognized that computer hacking is a

relatively new phenomenon, the indiscriminant use of

the term to refer to many different forms of unorthodox

computer use has been counterproductive to

understanding the extent of the activity. To avoid this

a "computer hacker" should be defined as an individual,

associated with the computer underground, who

specializes in obtaining unauthorized access to

computer systems. A "phone phreak" in an individual,

associated with the computer underground, who

specializes in obtaining unauthorized information about

the phone system. A "software pirate" is an

individual, associated with the computer underground,

who distributes or collects copyrighted computer

software. These definitions have been derived from the

data, instead of relying upon those who defend the

"integrity" of the original meanings, or those who are

unfamiliar with the culture.

    Topography of the Computer Underground

    Having defined the three main roles in the

computer underground, it is necessary to examine each

activity separately in order to provide a general

typology of the computer underground. In doing so, the

ways in which each contributes to the culture as a

whole will be illustrated, and the divisions between

them that affect the overall organization will be

developed. Analysis of these roles and divisions is

crucial to understanding identity, access, and mobility

within the culture.

Hacking

In the vernacular of the computer underground,

"hacking" refers to gaining access and exploring

computer systems and networks. "Hacking" encompasses

both the act and the methods used to obtain valid user

accounts on computer systems.

"Hacking" also refers to the activity that

occurs once access to another computer has been

obtained. Since the system is being used without

authorization, the hacker does not, generally speaking,

have access to the usual operating manuals and other

resources that are available to legitimate users.

Therefore, the hacker must experiment with commands and

explore various files in order to understand and

effectively use the system. The goal here is to

explore and experiment with the system that has been

entered. By examining files and, perhaps, by a little

clever programming, the hacker may be able to obtain

protected information or more powerful access

privileges.5

Phreaking

Another role in the computer underground is that

of the "phone phreak." Phone phreaking, usually called

just "phreaking," was widely publicized when the

exploits of John "Cap'n Crunch" Draper, the "father of

phreaking," were publicized in a 1971 Esquire magazine

article.

The term "phreaking" encompasses several different

means of circumventing the billing mechanisms of

telephone companies. By using these methods, long-
_____

     5 Contrary to the image sometimes perpetuated by
computer security consultants, the data indicate that
hackers refrain from deliberately destroying data or
otherwise damaging the system. Doing so would conflict
with their instrumental goal of blending in with the
average user so as not to attract undue attention to
their presence and cause the account to be deleted.
After spending what may be a substantial amount of time
obtaining a high access account, the hacker places a
high priority on not being discovered using it.

_____

distance phone calls can be placed without cost. In

many cases the methods also prevent, or at least

inhibit, the possibility of calls being traced to their

source thereby helping the phreaker to avoid being

caught.

     Early phreaking methods involved electro-

mechanical devices that generated key tones, or altered

line voltages in certain ways as to trick the

mechanical switches of the phone company into

connecting calls without charging. However the advent

of computerized telephone-switching systems largely

made these devices obsolete. In order to continue

their practice the phreaks have had to learn hacking

skills:6

     Phreaking and hacking have just recently
     merged, because now, the telephone companies
     are using computers to operate their network.
     So, in order to learn more about these
     computers in relation to the network, phreaks
     have learned hacking skills, and can now
     program, and get around inside the machines
     (AF, message log, 1988).

     For most members of the computer underground,

phreaking is simply a tool that allows them to call

long distance without amassing enormous phone bills.
_____

     6 Because the two activities are so closely
related, with phreakers learning hacking skills and
hackers breaking into "telco" computers, reference is
usually made to phreak/hacking or "p/hackers." This
paper follows this convention.

_____

Those who have a deeper and more technically oriented
interest in the "telco" (telephone company) are known
as phreakers. They, like the hackers discussed earlier,
desire to master and explore a system that few
outsiders really understand:

> The phone system is the most interesting,
> fascinating thing that I know of. There is so
> much to know. Even phreaks have their own
> areas of knowledge. There is so much to know
> that one phreak could know something fairly
> important and the next phreak not. The next
> phreak might know ten things that the first
> phreak doesn't though. It all depends upon
> where and how they get their info. I myself
> %sic% would like to work for the telco, doing
> something interesting, like programming a
> switch. Something that isn't slave labor
> bullshit. Something that you enjoy, but have
> to take risks in order to participate unless
> you are lucky enough to work for the telco.
> To have access to telco things, manuals, etc
> would be great (DP, message log, 1988).

> Phreaking involves having the dedication to
> commit yourself to learning as much about the
> phone system/network as possible. Since most
> of this information is not made public,
> phreaks have to resort to legally
> questionable means to obtain the knowledge
> they want (TP2, message log, 1988).

Most members of the underground do not approach
the telephone system with such passion. Many hackers
are interested in the phone system solely to the extent
that they can exploit its weaknesses and pursue other
goals. In this case, phreaking becomes a means and not
a pursuit unto itself. Another individual, one who
identifies himself as a hacker, explains:

> I know very little about phones . . . I just
> hack. See, I can't exactly call these numbers
> direct. A lot of people are in the same
> boat. In my case, phreaking is a tool, an
> often used one, but nonetheless a tool (TU,
> message log, 1988).

In the world of the computer underground, the
ability to "phreak a call" is taken for granted. The
invention of the telephone credit card has opened the
door to wide-scale phreaking. With these cards, no
special knowledge or equipment is required to phreak a

call, only valid credit card numbers, known as "codez,"

are needed to call any location in the world. This

easy access to free long-distance service is

instrumental for maintaining contact with CU

participants scattered across the nation.

Pirating

       The third major role in the computer underground

is that of the software pirate. Software piracy refers

to the unauthorized copying and distribution of copy-

righted software. This activity centers around

computer bulletin board systems that specialize in

"warez."7   There pirates can contribute and share
_____

       7 "Warez" is a common underground term that refers
to pirated software.

_____

copies of commercial software. Having access to these

systems (usually obtained by contributing a copyrighted

program via a telephone modem) allows the pirate to

copy, or "download," between two to six programs that

others have contributed.

       Software piracy is a growing concern among

software publishing companies. Some contend that the

illegal copying of software programs costs the industry

billions of dollars in lost revenues. Pirates challenge

this, and claim that in many ways pirating is a hobby,

much like collecting stamps or baseball cards, and

their participation actually induces them to spend more

on software than they would otherwise, even to the

point of buying software they don't truly need:

       There's a certain sense of, ahh, satisfaction
       in having the latest program, or being the
       first to upload a program on the "want list."
       I just like to play around with them, see
       what they can do. If I like something, I'll
       buy it, or try out several programs like it,
       then buy one. In fact, if I wasn't pirating,
       I wouldn't buy any warez, because some of

these I buy I do for uploading or just for
the fun of it. So I figure the software
companies are making money off me, and this
is pretty much the same for all the really
elite boards, the ones that have the best and
most programs. . . . I just bought a $117.
program, an accounting program, and I have
absolutely no use for it. It's for small
businesses. I thought maybe it would auto-
write checks, but it's really a bit too high
powered for me. I thought it would be fun to
trade to some other boards, but I learned a
lot from just looking at it (JX, field notes,
1989).

Pirates and phreak/hackers do not necessarily

support the activities of each other, and there is

distrust and misunderstanding between the two groups.

At least part of this distrust lies in the

phreak/hacker perception that piracy is an unskilled

activity.8 While p/hackers probably don't disapprove

of piracy as an activity, they nevertheless tend to

avoid pirate bulletin board systems --partly because

there is little pertinent phreak/hack information

contained on them, and partly because of the belief

that pirates indiscriminately abuse the telephone

network in pursuit of the latest computer game. One

hacker illustrates this belief by theorizing that

pirates are responsible for a large part of telephone

credit card fraud.

The media claims that it is solely hackers
who are responsible for losses pertaining to
large telecommunication companies and long
distance services. This is not the case. We
are %hackers% but a small portion of these
losses. The rest are caused by pirates and
thieves who sell these codes to people on the
street (AF, message log, 1988).

Other hackers complained that uploading large

_____

8 A possible exception to this are those pirates
that have the programming skills needed to remove copy
protection from software. By removing the program code
that inhibits duplicate copies from being made these
individuals, known as "crackers," contribute greatly to
the easy distribution of "warez."

_____

programs frequently takes several hours to complete,

and it is pirate calls, not the ones placed by "tele-

communications enthusiasts" (a popular euphemism for
phreakers and hackers) that cost the telephone industry
large sums of money. However, the data do not support
the assertation that all pirates phreak their calls.
Phreaking is considered "very tacky" among elite
pirates, and system operators (Sysops) of pirate
bulletin boards discourage phreaked calls because it
draws attention to the system when the call is
discovered by the telephone company.

Regardless of whether it is the lack of phreak/
hack skills, the reputation for abusing the network, or
some other reason, there is indeed a certain amount of
division between the world of phreakers and hackers and
that of pirates. The two communities co-exist and share
resources and methods, but function separately.

Social Organization and Deviant Associations

Having outlined and defined the activities of the
computer underground, the question of social
organization can be addressed. Joel Best and David
Luckenbill (1982) have developed a typology for
identifying the social organization of deviant
associations. Essentially they state that deviant
organizations, regardless of their actual type of
deviance, will vary in the complexity of their division
of labor, coordination among organization roles, and
the purposiveness with which they attempt to achieve
their goals. Those organizations which display high
levels in each of these categories are more
sophisticated than those with lower levels.

          Deviants relations with one another can be
     arrayed along the dimension of organizational
     sophistication. Beginning with the least
     sophisticated form, %we% discuss five forms
     of the social organization of deviants:
     loners, colleagues, peers, mobs, and formal
     organizations. These organization forms are
     defined in terms of four variables: whether
     the deviants associate with one another;

whether they participate in deviance
together; whether their deviance requires an
elaborate division of labor; and whether
their organization's activities extend over
time and space (Best and Luckenbill, 1982,
p.24).

These four variables, also known as mutual association,

mutual participation, elaborate division of labor, and

extended organization, are indicators of the social

organization of deviant groups. The following, taken

from Best and Luckenbill, illustrates:

```
FORM OF        MUTUAL     MUTUAL      DIVISION  EXTENDED
ORGAN-         ASSOCIA-   PARTICIPA-  OF        ORGAN-
IZATION        TION       TION        LABOR     IZATION
-----------------------------------------------------
Loners         no         no          no        no
Colleagues     yes        no          no        no
Peers          yes        yes         no        no
Mobs           yes        yes         yes       no
Formal
Organizations  yes        yes         yes       yes
_____
                                       (1982, p.25)
```

Loners do not associate with other deviants,
participate in shared deviance, have a
division of labor, or maintain their deviance
over extended time and space. Colleagues
differ from loners because they associate
with fellow deviants. Peers not only
associate with one another, but also
participate in deviance together. In mobs,
this shared participation requires an
elaborate division of labor. Finally, formal
organizations involve mutual association,
mutual participation, an elaborate division
of labor, and deviant activities extended
over time and space (Best and Luckenbill,
1982, pp.24-25).

The five forms of organizations are presented as

ideal types, and "organizational sophistication" should

be regarded as forming a continuum with groups located

at various points along the range (Best and Luckenbill,

1982, p.25). With these two caveats in mind, we begin

to examine the computer underground in terms of each of

the four organizational variables. The first level,

mutual association, is addressed in the following

section.

Mutual Association

Mutual association is an indicator of

organizational sophistication in deviant associations.

Its presence in the computer underground indicates that

on a social organization level phreak/hackers act as

"colleagues." Best and Luckenbill discuss the

advantages of mutual association for unconventional

groups:

> The more sophisticated the form of
> organization, the more likely the deviants
> can help one another with their problems.
> Deviants help one another in many ways: by
> teaching each other deviant skills and a
> deviant ideology; by working together to
> carry out complicated tasks; by giving each
> other sociable contacts and moral support; by
> supplying one another with deviant equipment;
> by protecting each other from the
> authorities; and so forth. Just as %others%
> rely on one another in the course of everyday
> life, deviants find it easier to cope with
> practical problems when they have the help of
> deviant associates (1982,pp.27-28).

Hackers, phreakers, and pirates face practical

problems. For example, in order to pursue their

activities they require equipment9 and knowledge. The
_____

9 The basic equipment consists of a modem, phone
line, and a computer -- all items that are available
through legitimate channels. It is the way the
equipment is used, and the associated knowledge that is
required, that distinguishes hackers from other
computer users.

_____

problem of acquiring the latter must be solved and,

additionally, they must devise ways to prevent

discovery , apprehension and sanctioning by social

control agents.10

One method of solving these problems is to turn to

other CU members for help and support. Various means

of communication have been established that allow

individuals to interact regardless of their location.

As might be expected, the communication channels used

by the CU reflect their interest and ability in high-

technology, but the technical aspects of these methods

should not overshadow the mutual association that they

support. This section examines the structure of

mutual association within the computer underground.
_____

      10 Telephone company security personnel, local law
enforcement, FBI, and Secret Service agents have all
been involved in apprehending hackers.

_____

        The Structure of the Computer Underground

        Both computer underground communities, the

p/hackers and the pirates, depend on communications

technology to provide meeting places for social and

"occupational" exchanges. However, phreakers, hackers,

and pirates are widely dispersed across the country

and, in many cases, the globe. In order for the

communication to be organized and available to

participants in many time zones and "working" under

different schedules, centralized points of information

distribution are required. Several existing

technologies --computer bulletin boards, voice mail

boxes, "chat" lines, and telephone bridges/loops --

have been adopted by the CU for use as communication

points. Each of these technologies will be addressed in

turn, giving cultural insight into CU activities, and

illustrating mutual association among CU participants.

Bulletin Board Systems

        Communication in the computer underground takes

place largely at night, and primarily through Bulletin

Board Systems (BBS). By calling these systems and

"logging on" with an account and password individuals

can leave messages to each other, download files and

programs, and, depending on the number of phone lines

into the system, type messages to other users that may

be logged on at the same time.

        Computer Bulletin Board Systems, or "boards," are

quite common in this computerized age. Nearly every
medium-sized city or town has at least one. But not all
BBS are part of the computer underground culture.   In
fact, many systems prohibit users from discussing CU
related activity. However, since all bulletin boards
systems essentially function alike it is only the
content, users, and CU culture that distinguish an
"underground" from a "legitimate" bulletin board.

     Computer Underground BBS are generally owned and
operated by a single person (known as the "system
operator" or "sysop"). Typically setup in a spare
bedroom, the costs of running the system are paid by
the sysop, though some boards solicit donations from
users. The sysop maintains the board and allocates
accounts to people who call the system.

     It is difficult to assess the number of
underground bulletin boards in operation at any one
time. BBS in general are transitory in nature, and CU
boards are no exception to this. Since they are
operated by private individuals, they are often set up
and closed down at the whim of the operator. A week
that sees two new boards come online may also see
another close down. A "lifetime" of anywhere from 1
month to 1-1/2 years is common for pirate and
phreak/hack boards.11   One BBS, claimed to be the
"busiest phreak/hack board in the country" at the
time,12 operated for less than one year and was
suddenly closed when the operator was laid off work.

     Further compounding the difficulty of estimating
the number of CU boards is their "underground" status.
CU systems do not typically publicize their existence.
However, once access to one has been achieved, it is
easy to learn of other systems by asking users for the
phone numbers. Additionally, most BBS maintain lists

of other boards that users can download or read. So it

is possible, despite the difficulties, to get a feel

for the number of CU boards in operation.   Pirate

boards are the most common of "underground" BBS. While

there is no national "directory" of pirate boards,

there are several listings of numbers for specific
_____

        11 While some non-CU BBS' have been operating
since 1981, the longest operating phreak/hack board has
only been in operation since 1984.

        12 At it's peak this p/h board was receiving 1000
calls a month and supported a community of 167 users
(TP BBS, message log, 1989).

_____

computer brands.13 One list of Apple pirate boards has

700 entries. Another, for IBM boards, lists just over

500. While there is no way of determining if these

lists are comprehensive, they provide a minimum

estimate. Pirate boards for systems other than IBM or

Apple seem to exhibit similar numbers. David Small, a

software developer that has taken an aggressive stance

in closing down pirate boards, estimates that there are

two thousand in existence at any one time (1988).

Based on the boards discovered in the course of this

research, and working from an assumption that each of

the four major brands of microcomputers have equal

numbers of pirate boards, two thousand is a reasonable

estimate.

        The phreak/hack BBS community is not divided by

differing brands of micro-computers. The applicability

of phreak/hack information to a wide range of systems

does not require the specialization that pirate boards

exhibit. This makes it easier to estimate the number

of systems in this category.

        John Maxfield, a computer security consultant, has

asserted that there are "thousands" of phreak/hack

_____

     13 Pirate boards are normally "system specific" in
that they only support one brand or model of
microcomputer.
_____

boards in existence (WGN-Radio, November 1988). The

data, however, do not confirm this. A list of

phreak/hack boards compiled by asking active p/hackers

and downloading BBS lists from known phreak/hack

boards, indicates that there are probably no more than

one hundred. Experienced phreak/hackers say that the

quality of these boards varies greatly, and of those

that are in operation today only a few (less than ten)

attract the active and knowledgeable user.

     Right after "War Games" came out there must
     have been hundreds of hacker bulletin boards
     spring up. But 99% of those were lame. Just a
     bunch of dumb kids that saw the movie and
     spent all there %sic% time asking "anyone got
     any k00l numberz?" instead of actually
     hacking on anything. But for a while there
     was %sic% maybe ten systems worth calling . .
     . where you could actually learn something
     and talk to people who knew what was going
     Nowadays %sic% there are maybe three that I
     consider good . . . and about four or five
     others that are okay. The problem is that
     anybody can set up a board with a k-rad name
     and call it a hacker board and the media/feds
     will consider it one if it gets busted. But
     it never really was worth a shit from the
     beginning.(TP2, field notes, 1989)

     Towards a BBS Culture. Defining and identifying

CU boards can be problematic. The lack of an ideal

type undoubtedly contributes to the varying estimates

of the number of CU bulletin board systems. While

developing such a typology is not the intent of this

work, it is appropriate to examine the activities and

characteristics exhibited by BBS supporting the pirate

and phreak/hack communities. While much of the culture

of pirate and phreak/hack worlds overlap, there are

some differences in terms of how the BBS medium is used

to serve their interests. We begin with a short

discussion of the differences between the two

communities, then discuss cultural characteristics
common to all CU BBS systems.

All BBS feature a "files area" where programs and
text files are available for downloading by users.
Initially these programs/files are supplied by the
system operator, but as the board grows they are
contributed (called "uploading") by callers. The
content and size of the files area differs according to
whether the board supports the pirate or phreak/hack
community.

The files area on a pirate board consists
primarily of programs and program documentation.
Normally these programs are for only one brand of
micro-computer (usually the same as the system is being
run on). Text files on general or non-computer topics
are uncommon. A "files area" menu from a pirate BBS
illustrates the emphasis on software:

```
%1% Documentation        %2% Telecommunications
%3% Misc Applications    %4% Word Processing
%5% Graphics             %6% Utilities
%7% Games 1              %8% Games 2
%9% XXX Rated            %10% Elite_1
%11% Elite_2             %12% Super_Elite
                    (IN BBS, message log, 1988)
```

The "files area" on a phreak/hack BBS is
noticeably smaller than it is on pirate systems. It
consists primarily of instructional files (known as "g-
files" for "general files") and copies of phreak/hack
newsletters and journals. Pirated commercial software
is very rare; any programs that are available are
usually non-copyrighted specialized programs used to
automate the more mundane aspects of phreaking or
hacking. It is not uncommon to find them in forms
usable by different brands of computers. A "files
area" list from a phreak/hack BBS is listed here
(edited for size):

        Misc Stuff

```
             -------------
             BRR2    .TXT: Bell Research Report Volume II
             BRR1    .TXT: Bell Research Report Volume I
             CONFIDE .ARC: Confide v1.0 DES
                           EnCryption/DeCryption
             CNA     .TXT: A bunch of CNA numbers
             CLIPS   .ARC: newsclippings/articles on hackers
                           and busts
             ESS1    .TXT: FILE DESCRIBING THE ESS1 CHIP
             TELEPHON.TXT: NY Times Article on hackers/phreaks
             HP-3000 .TXT: This tells a little info about hp
             VIRUS   .TXT: Digest of PC anti-viral programs.

             Hack/Phreak Programs
             -----------------------
             THIEF   .ARC: Code Thief for IBM!
             PC-LOK11.ARC: IBM Hard Disk Lock Utility- fairly
                           good.
             PHONELIS.COM: Do a PHONE DIR command on VAX from
                           DCL.
             XMO     .FOR: VAX Xmodem Package in FORTRAN
             PASSWORD.ARC: IBM Password on bootup.  Not too
                           bad.

             Archived Gfiles
             ---------------------
             PHRACK15.ARC: Phrack #15
             PHRACK10.ARC: Phrack #10
             PHRACK20.ARC: Phrack #20
             ATI1_6.ARC  : ATI issues one thru six
             PHRACK5.ARC : Phrack #5
             PHRACK25.ARC: Phrack #25
             PHUN1.ARC   : P/Hun first issue
             TCSJ.ARC    : Telecom Security Journal
             ATI31.ARC   : Activist Times Inc number 31
             LODTECH3.ARC: LoD Tech Journal three
                                 (TPP BBS, message log, 1988)
```

The difference in files area size is consistent

with the activities of pirates and phreak/hackers. The

main commodity of exchange between pirates is, as

discussed earlier, copyrighted software thus accounting

for the heavy use of that area of the board that

permits exchange of programs. The phreak/hackers, on

the other hand, primarily exchange information about

outside systems and techniques. Their interests are

better served by the "message bases" of BBS.

The "message bases" (areas where callers leave

messages to other users) are heavily used on

phreak/hack systems. The messages are not specific to

one brand of micro-computer due to the fact that not

all users own the same equipment. Rather than focus on

the equipment owned by the phreak/hacker, the messages

deal with their "targets." Everything from

phreak/hacking techniques to CU gossip is discussed. On

some boards all the messages, regardless of topic, are

strung together in one area. But on others there are

separate areas dealing with specific networks and

mainframe computers:

```
     Message Boards available:

      1 : General
      2 : Telecommunications
      3 : Electronics
      4 : Packet Switched Nets
      5 : VAX/DEC
      6 : Unix
      7 : Primos
      8 : HP-x000
      9 : Engineering
     10 : Programming & Theory
     11 : Phrack Inc.
     12 : Sociological Inquiries
     13 : Security Personnel & Discussion
     14 : Upper Deck
     15 : Instructors
                          (TPP BBS, message log, 1988)
```

The pirate community, on the other hand, makes

little use of the "message bases." Most users prefer to

spend their time (which may be limited by the system

operator on a per day or per call basis) uploading

and/or downloading files rather than leaving messages

for others. Those messages that do exist are usually

specific to the pirating enterprise such as help with

programs on the board, requests for specific programs

("want lists"), and notices about other pirate bulletin

boards that users may want to call. Occasional

discussion of phreaking may occur, but the emphasis is

on techniques used to make free calls, not technical

network discussions as often occurs on phreak/hack

systems. A list of message areas from a large pirate

BBS illustrates the emphasis on the pirating

enterprise. A message area for general discussions has

been created, but those areas devoted to pirating

display more use:

```
            Area %1% General Discussion       15 messages
            Area %2% Pirating Only!!          75 messages
            Area %3% Warez Wants             31 messages
            Area %4% **private messages**    10 messages
                         (TL BBS, message log, 1988)
```

In addition to the differences between files and
message use on pirate and phreak/hack boards, they
differ in degree of community cohesiveness. Every BBS
has a group of "users" --the people who have accounts
on the system. The group of users that call a specific
BBS can be considered to be a "community" of loosely
associated individuals by virtue of their "membership"
in the BBS.

Additionally, the system itself, serving either
pirates or phreak/hackers, exists within a loose
network of other bulletin boards that serve these same
interests. It is within this larger community where
pirate and phreak/hack boards seem to differ.

Due to the brand-specific nature of pirate boards,
there is not a strong network between pirate BBS that
operate on other systems. This is understandable as a
pirate that owned an Apple computer would have little
use for the programs found on an IBM board. However,
this creates separate communities of active pirates,
each loosely associated with other users of their
computer type, but with little or no contact with
pirate communities on other systems.

There is, however, a degree of cohesiveness among
pirate boards that support the same micro-computers.
While the users may be different on systems, the data
shows that some pirate boards are "networked" with each
other via special software that allows messages and
files to be automatically shared between different
boards. Thus a message posted on a west coast pirate
board will be automatically copied on an east coast BBS
later that night. In a like manner, software programs

can be sent between "networked" boards. The extent of
this network is unknown.

The pirate BBS community also exhibits
cohesiveness in the form of "co-sysops." As discussed
earlier, sysops are the system operators and usually
owners of BBS. On some pirate boards, "co-sysop"
distinction is given to an operator of another board,
often located in another state. This forms a loose
network of "sister boards" where the sysop of one has
co-sysop privileges on the other.   However, this
cooperative effort appears to be limited mainly to the
system operators as comparing user lists from sister
boards shows little overlap between the regular
callers. How co-sysop positions are utilized is
unknown, and it is suspected that they are largely
honorary. But nonetheless it is indicative of mutual
association between a small number of boards.

The phreak/hack board community does not exhibit
the same brand-specific division as the pirate
community. Unlike the divided community of pirates,
phreak/hackers appear to maintain contacts throughout
the country. Obtaining and comparing user lists from
several phreak/hack BBS reveals largely the same group
of people using several different boards across the
country.14 While phreak/hack boards have yet to adopt
the "networking" software used by pirate boards, an
active group of phreak/hackers is known to use the
sophisticated university mainframe computer network,
called Bitnet, to exchange phreak/hack newsletters and
gossip.

Despite the operational differences between pirate
_____

14 In fact, users lists from phreak/hack BBSs
located in Europe and Australia show that many U.S.
p/hackers utilize these systems as well.

_____

and phreak/hack boards, their cultures are remarkably

similar. Any discussion of the computer underground

must include both communities. Additionally, a

formulation of the culture of CU BBS must address the

means in which access to the board, and thus deviant

associates, is obtained.

    For a caller to successfully enter the CU BBS

community, he must display an awareness of CU culture

and technical skill in the CU enterprise. If the caller

fails to exhibit cultural knowledge, then access to the

board is unlikely to be granted. The ways in which

this cultural knowledge is obtained and displayed

illustrates the social nature of the CU and further

displays some of the subcultural norms of behavior.

    On most "licit" (non-underground) boards,

obtaining permission to use the system is accomplished

by logging on and providing a name and home phone

number to the system operator (sysop). Sysop's

normally do not check the validity of the information,

and once a caller has provided it he or she is granted

full access to the system. There is normally one level

of access for all users, with only the sysop having

more "powerful" access.

    Obtaining access to underground bulletin boards is

more complicated and requires more steps to complete.

In an attempt to prevent law enforcement agents

("feds") from obtaining accounts on systems where

pirates or p/hackers are vulnerable, if not to actual

arrest, then at least to exposing their latest act-

ivities and methods, sysop's of illicit boards attempt

to limit access to the system.

    One method of doing this is to restrict

publicizing the existence of the board. Computer

underground BBS are not normally included in BBS
listings found in computer books and magazines, and
there is a norm, particularly strong on p/hack systems,
that the boards are not to be mentioned on non-CU
systems. There are, however, some "entry-level" CU BBS
that are fairly well known. These systems are known as
"anarchist" boards.

"Anarchist" boards, while exhibiting many of the
same characteristics as pirate and phreak/hack boards,
are really a cross between the two and serve primarily
as social outlets for both pirates and phreak/hackers.
The message areas on "anarchist" boards are quite
active, "chatty" messages are not discouraged. Indeed
there are normally several different message areas
devoted to a wide range of topics including everything
from "skipping school" to "punk rock." The files area
contains both warez (but normally only the newest
games, and specific to the computer system that the
board runs on) and phreak/hack text files. Neither

collection is as extensive as it would be on pirate-
only or p/hack-only systems.

The data suggest that one function of "anarchist"
boards is to introduce newcomers to the culture of the
computer underground. By acting as "feeder boards,"
they can provide preliminary socialization and
instruction for CU behavior and techniques.
Additionally, "anarchist" boards frequently provide
areas where phone numbers to pirate and p/hack systems
can be traded, thus providing systems where more in-
depth information, and other contacts, can be found. A
phreak/hacker describes how an "anarchist" board was
instrumental in introducing him to the computer
underground:

I've been phreaking and hacking for about

four years now. I discovered phreaking on my
own at this place I used to work. We had
this small LD %long distance% provider that
used codez so I started hacking them out and
calling places myself . . . but I didn't know
no other phreaks at that time. Then I
started using the codez to call boards from
home on my computer. Somebody gave me the
number to Jack Black's Whore House %an
"anarchy board"% and I started learning about
hacking and shit from the people and philes
they had there. Then one day this guy, King
Hammer, sent me some e-mail %a private
message% and told me to call his system.
That's where I really learned my way around
the nets and shit. You could ask questions
and people would help you out and stuff. If I
hadn't found out some of the tricks that I
did I probably would have got busted by now.
(TP2, field notes, 1989)

Once an individual has obtained the telephone

number to a CU BBS, through whatever channels, callers

follow essentially the same procedure as they do on

licit systems . . . that of calling and logging on.

However, since "underground" boards are not truly

underground (that is, totally secret) first-time

callers are not given access to the board itself. When

a user is unable to provide an already valid

username/password, the system will automatically begin

its registration procedure.   First, the caller is

asked to enter a "username" (the name used by the

system to distinguish between callers) and "phone

number."   These first system requests, normally seen

only as "Enter Your Name and Phone Number," serve as

partial screens to keep out non-underground callers

that may have happened across the board. The way that

a user responds to these questions indicates if they

have cultural knowledge of the CU. The norm is to

enter a pseudonym and a fake phone number.15 If a
_____

15 A functional reason for this norm is that
usernames and telephone numbers are stored on the
computer as part of the BBS system files. Should the
BBS ever be seized in legal proceedings, this list of
names and numbers (and on some systems addresses . . .
which are also normally false) could be used to
identify the users of the system.
_____

caller enters his or her real name (or at least a name
that does not appear to be a pseudonym) the system
operator will be put on guard that the caller may not
be aware of the type of board that he has called, for
the pseudonym is the most visible of CU cultural
traits.

     All members of the underground adopt "handles" to
protect their identity. The pseudonyms become second
identities and are used to log onto bulletin boards,
and as "signatures" on messages and instructional text
files.16 They are not unlike those adopted by
citizens-band radio users, and reflect both the humor
and technical orientation of computer underground
participants. A review of handles used by phreakers,
hackers, and pirates finds that they fall into three
broad categories: figures from literature, films, and
entertainment (often science fiction); names that play
upon computers and related technologies; and
nouns/descriptive names. (See Appendix A for fictional
examples of each.)

     After providing a user name and entering a

_____

     16 The data suggest that, on the whole,
individuals retain their handles over time.
_____

password to be used for future calls, the caller is
asked several more questions designed to screen users
and determine initial access privileges. Unlike licit
boards, underground BBS may have several different
levels of access with only the most trusted users being
able to read messages and get files in "elite" or "high
access" areas that are unknown and unavailable to other
callers. In many cases, pirate boards are able to
operate "above ground" and appear to be open-public
access systems unless callers have the proper

privileges to access the areas where the "good stuff"

is located. The answers given to access questionnaires

determine whether a caller will receive access to some,

all, or none of the higher levels.

These questionnaires frequently ask for "personal

references" and a list of other boards the caller has

"high access" on. The question is vague, and random

callers are unlikely to answer it correctly. However,

if the caller lists pseudonyms of other CU members that

are known and trustworthy to the sysop, as well as some

other boards that are known to have "good users" and

"good security" access will usually be granted.17   If

all the answers are relevant and indicative of CU

_____

17 The data suggest that personal references are
only checked if something seems unusual or suspicious.
_____

knowledge, then initial access is normally granted.

Other methods of controlling access include

presenting a "quiz" to determine if the technical

knowledge of the user is up to par with the expertise

expected on the boards.18 Some systems, instead of a

quiz, ask the user to write a short statement (100

words or less) about why they want access, where they

got the phone number to the system, and what they can

provide to other users. Some pirate boards come right

out and ask the user to supply a list of the good

"warez" that they can upload and what they are looking

to download. If the caller fails to list recent

copyrighted programs then it is evident that they are

unaware of the nature of the BBS:

    I had this one dude call up and he told me in
    his message that he was looking for some
    "good games." So instead of giving him
    access I just left him some e-mail %a private
    message%. I asked what kind of games he was
    looking for. Next time he called he wrote
    back and said "a public domain Asteroids
    game." I couldn't believe it. Not only is

                    Asteroids so damn old it's lame, but this guy
                    is looking for pd %public domain% shit. No
                    way was he going to get access. He didn't
                    even know what this board is. I left him a
                    message telling him that I didn't have one.
                    He never called back after that (CH, sysop of
                    a pirate BBS, field notes, 1988).

        _____

            18 One such quiz, from a p/h board, can be found
        in Appendix B.
        _____

            Ironically, the pseudo-elaborate security methods

        of underground boards, while they may be effective in

        keeping off random non-CU callers, are not effective in

        screening out "feds." Data and media accounts show that

        boards are regularly infiltrated by telephone security

        personnel and software companies. Also, the adoption of

        handles to protect identities is defeated by the

        consistent use of the same handle over time. But in

        order to obtain and maintain status and prestige in the

        CU one must keep the same pseudonym in order to

        (literally) "make a name for oneself." The fact that CU

        communication is not face-to-face requires a consistent

        means of identifying oneself to others. The handle

        fulfills this purpose but at the same time becomes as

        attached to a single individual as a real name would.

        The access rituals of the computer underground, which

        are contingent on being a "known" pirate or

        phreak/hacker, make changing handles unproductive.

            The life blood and center of the computer under-

        ground is the bulletin board network. Acting as both

        the main trade center of performance related tools and

        innovations and as a means of socialization, the

        underground could not exist without the BBS network.

        They serve to "recruit" and educate newcomers and

        provide a way to traffic in information and software.

        The pirating enterprise in particular is very dependent

        upon the BBS as they are the very means by which

"warez" are traded. For the phreak/hacker community,
BBS provide a means of trading the resources of system
numbers and passwords, as well as instructional texts
on techniques. The access process serves as evidence
of mutual association amongst phreakers, hackers, and
pirates as cultural knowledge is needed as well as
personal references (evidence of acceptance and access
to others).

   The CU bulletin board systems are unique in that
they provide a way to exchange information with a large
number of others. The other methods of CU commun-
ication are based on conversations rather than written
texts and thus are much less permanent. These methods,
discussed next, are telephone bridges/loops, voice mail
boxes, and computer "chat" systems.

Bridges, Loops, and Voice Mail Boxes
   Of the additional means of communication used by
the CU, telephone "bridges" and "loops" are most
common. Unlike BBS, which require data links provided
by a computer and modem, bridges and loops are "old
fashioned" voice connections. Since they can not
accommodate the transfer of programs or files they are
used primarily by phreakers and hackers, and most often
as a social/recreational outlet.

   A "bridge" is a technical name for what is
commonly known as a "chat line" or "conference system."
They are familiar to the public as the pay-
per-minute group conversation systems advertised on
late night television. Many bridge systems are owned
by large corporations who maintain them for business
use during the day. While the numbers to these systems
is not public knowledge, many of them have been
discovered by phreaks who then utilize the systems
during the night.

In addition to these pre-existing conference

systems, phreakers have become skilled at arranging

for a temporary, private bridge to be created via

AT&T's conference calling facilities. This allows for

conversations to be held among a self-selected group of

phreak/hackers:19

>   Bridges can be %sic% extremely useful means
>   of distributing information as long as the
>   %phone% number is not known, and you don't
>   have a bunch of children online testing out

_____

19 The data indicates that these private
conference calls aren't "scheduled" in any real sense.
One p/hacker will initiate the conference and call
others at home to add them to the conference. As more
people join they suggest others to add. The initiator
can temporarily jump out of the conference, call the
new person and solicit their attendance. If they don't
want to join or aren't home, the initiator simply
returns to the conference without adding them in.

_____

>   their DTMF.20 The last great discussion I
>   participated with over a bridge occurred
>   about 2 months ago on an AT&T Quorum where
>   all we did was engineer 3/way %calls% and
>   restrict ourselves to purely technical infor-
>   mation. We could have convinced the Quorum
>   operators that we were AT&T technicians had
>   the need occurred. Don't let the kids ruin
>   all the fun and convenience of bridges.
>   Lameness is one thing, practicality is
>   another (DC, message log, 1988).

In addition to setting up "private" bridges,

p/hackers can utilize "loop lines" in a further attempt

to limit the number of eavesdroppers on their

conversations. Unlike bridges, which connect a

virtually unlimited number of callers at once, "loops"

are limited to just two people at a time.

"Loop lines" are actually telephone company test

lines installed for internal use.21 A loop consists of

two separate telephone numbers that connect only to

each other. Each end has a separate phone number, and

when each person calls one end, they are connected to

each other automatically. This allows for individuals

_____

20 "Dual Tone Multi Frequency" or in laymen terms,
the touch tone sounds used to dial phone numbers.

21 These test lines are discovered by phreaks and
hackers by programming their home computer to dial
numbers at random and "listen" for the distinctive tone
that an answering loop makes, by asking sympathetic
telephone company employees, or through information
contained on internal company computers.
_____

to hold private conversations without divulging their

location or identity by exchanging telephone numbers.

Finally, voice mail boxes ("VMB") are another

means of communicating with individual actors. There

are several commercial voice mail box systems located

throughout the country. They function similar to a

telephone answering machine in that callers can call

in, listen to a recorded message, and then leave a

message for the box owner. Many of these systems are

accessible via toll-free telephone numbers. The

security of some VMB systems is notoriously poor. Many

phreaks have expertise in "creating" boxes for

themselves that are unknown (until discovered) by the

owner of the system. However, these boxes are usually

short lived since discovery by the system operator, and

closure of the box, is only a matter of time. But as

long as the box is functioning, it can serve as a means

of communicating with others. VMB numbers are

frequently posted on bulletin boards with invitations

to "call if you have any good stuff." They are often

used by pirates to exchange messages about new releases

of software, and by phreak/hackers to trade account and

access numbers. Additionally, some of the underground

newsletters and journals obtain boxes so users can call

in news of arrests and other gossip.

Like bulletin boards, VMBs are systems that allow

information to be disseminated to a large number of

associates, and unlike the live telephone conversations

of bridges and loops, they are available at any time of
the day. Additionally, VMB's don't require use of a
computer and modem, only a touch tone phone is needed
to call the box. Their usefulness is limited somewhat
because they play only one "outgoing" message at a
time, and their transitory nature limits their
reliability.

Summary

      Phreakers, hackers and pirates do not act as
loners. They have adopted existing methods of
communication, consistent with their skills in high
technology, to form a social network that allows for
the exchange of information, the socialization of new
members, socializing with others, and in the case of
pirates, performing the "deviant" act itself via these
means.

      These communication points create and foster
groups of loosely associated individuals, with specific
interests, coming together to exchange information
and/or software. It is impossible to be a part of the
social network of the computer underground and be a
loner.   Based upon the Best and Luckenbill measure,
actors in the computer underground, by displaying
mutual association, organize as colleagues.

      The social network of the computer underground
provides the opportunity for colleagues to form
cooperative working relationships with others, thus
moving the CU towards a more sophisticated form of
social organization. These "hacker groups" are
addressed in the next section.

Mutual Participation

      In the previous chapter the ways in which the
structure of the computer underground fosters mutual

association were discussed. Their social outlets and

means for informational exchange bring the CU community

together as deviant colleagues. Their relationships

fit quite well into the Best and Luckenbill (1982)

typology of collegial associations:

> The relationship between deviant colleagues
> involves limited contact. Like loners,
> colleagues perform their deviant acts alone.
> But unlike loners colleagues associate with
> one another when they are not engaged in
> deviance . . . In effect, there is a division
> between two settings; onstage where
> individual performs alone; and backstage,
> where colleagues meet (cf Goffman). In their
> backstage meetings, colleagues discuss
> matters of common interest, including
> techniques for performing effectively, common
> problems and how to deal with them, and ways
> of coping with the outside world (1982 p.37).

However, despite the advantages of collegial

association, ties between CU participants are weak.

Loyalty between individuals seems rare, as the CU is

replete with tales of phreak/hackers who, when

apprehended, expose identities or "trade secrets" in

order to avoid prosecution. These weak collegial ties

may be fostered by the anonymity of CU communication

methods, and the fact that all CU actors are, to some

extent, in competition with each other. There are only

so many systems with weak security and once such a

system is found, sharing it with others will virtually

ensure that the hole will be sealed when the increased

activity is noticed. Thus while p/hackers will share

general knowledge with each other, specific information

is not disseminated publicly.

As Best and Luckenbill have observed, in order to

remain in a collegial relationship individuals must be

able to successfully carry out operations alone (1982

p.45). In order to sustain a career in p/hacking one

must pursue and collect information independent of what

is shared on the communication channels. Despite the

association with other phreakers and hackers, the

actual performance of the phreak/hacking act is a

solitary activity.22

     That is not to say, however, that p/hackers never

share specific information with others. As discussed

earlier, p/hack bulletin board systems frequently have

differentiated levels of access where only highly

regarded individuals are able to leave and read

messages. These areas are frequently used to keep
_____

     22 This does not hold true for pirates. By
definition they must trade programs with other
individuals.
_____

information from "unskilled" users at the lower levels.

There are strong social norms that some information

should not be shared too widely, as it may be either

"abused" or fall into the hands of enforcement agents.

For example, when one p/hacker announced that he was

going to release a tutorial on how to infiltrate a new

telephone company computer, he received the following

messages in reply:

> Not smart, DT. %That computer% is a system
> which can be quite powerful if used to its
> potential. I don't think that information on
> programming the switches should be released
> to anyone. Do you realize how destructive
> %that computer% could really be if used by
> someone who is irresponsible and intends on
> destroying things? Don't even think about
> releasing that file. If you do release that
> file, it will disappear and will no longer
> remain in circulation. Believe me. Not many
> have the right to know about %that computer%,
> or any other delicate telco computers for
> that matter. Why do you think the fucking New
> York Times published that big article on
> hackers screwing around with telco machines?
> Not only will you get into a lot of trouble
> by releasing that file on %computer%, you
> will be making telcos more aware of what is
> actually happening, and soon no one will be
> able to learn about their systems. Just think
> twice (EP, message log, 1988).
>
> Why would you want normal people to have such
> knowledge? Any why would you post about it?
> If you have knowledge that's fine but DON'T
> spread that knowledge among others that may
> abuse it. It's not impressive! I don't know
> why anyone would want to disperse that

knowledge. Please don't release any "in
depth" files on such systems of great power.
Keep that to yourself it will just mess it up
for others (UU, message log, 1988).

The desire to share information with selected

colleagues often leads to the formation of cooperative

"working groups." These partnerships are easily formed,

as the structure of mutual association in the CU

creates a means where "talent" can be judged on the

basis of past interactions, longevity in the field, and

mutual interests. When allegiances are formed, the CU

actors begin "mutual participating" in their acts, thus

becoming "peers" in terms of social organization.

Mutual participation, as defined in the Best and

Luckenbill typology, is exhibited by actors sharing in

the same deviant act, in the physical presence of one

another (1982 p.45). However, the measurement was

"grounded" in studies of traditional deviant

associations (eg: street gangs, prostitutes, etc.)

where "real-time" interaction is common. The technology

used by the CU negates this requirement as actors can

be located in different parts of the country.

Additionally, "hacking" on a system, by a group of

peers, does not require simultaneous participation by

all members. However Best and Luckenbill's typology is

an ideal type, and the activities of peers in the

computer underground do not fall outside of the spirit

or intention of their concept of mutual participation.

Their description of deviant peer associations is

presented here:

Deviant peers are distinguished from
colleagues by their shared participation in
deviance. While colleagues carry out their
deviant operations alone, peers commit
deviant acts in one another's presence.
Peers cooperate in carrying out deviant
operations, but they have a minimal division
of labor, with each individual making roughly
comparable contribution. Peer relationships
also tend to be egalitarian and informal;
some peers may be acknowledged leaders or

admired for their skill, but there is no set
division of authority. Like colleagues,
peers share subcultural knowledge, but peer
groups typically provide their members with
more support. In addition to cooperating in
deviant operations, peers may recruit and
socialize newcomers and supply one another
with deviant equipment and social support.
Thus, the bonds between peers are stronger
than those linking colleagues (1982, p.45).

Peer associations in the CU are largely limited to

small groups23 working on a specified goal. Both

pirates and p/hackers organize themselves in this

regard, though their characteristics differ. We begin

with a discussion of mutual participation among

pirates.

Pirate Groups

Pirate groups are composed of less than ten
_____

23 In terms of the ideal type for deviant peers
any two individuals working in cooperation exhibit
mutual participation. The discussion here addresses
groups that consist of three or more people that
identify themselves as a sort of "club." Short-lived
interaction between two people is not considered a
"group" in the CU culture.
_____

members. Their primary purpose is to obtain the latest

software, remove any copy-protection from it, and then

distribute it to the pirate community. Often the

"warez" that they distribute will be adorned with the

group name, so subsequent users will be aware of the

source of the software. Many pirate groups have "home"

BBS systems that act as key distribution points, and as

places where outsiders can communicate with members of

the association. This researcher was unable to obtain

data about the internal organization of pirate groups,

but it appears that they are leaderless, with

individual members working alone but giving credit to

the group as a whole.

Phreak/hack groups
The existence of phreak/hacker groups is well

documented in the data, and has been heavily reported
in the media. Two hacker groups in particular, The
414's (named for the Wisconsin area code in which they
lived), and The Inner Circle, received a large amount
of press after being apprehended for various computer
break-ins. However, the "threat" that such groups
represent has probably been overstated as the data
indicate that "hacker gangs" vary greatly in
organization and dedication to the CU enterprise.

Many hacker groups are short-lived associations of
convenience, much like the "no girls allowed!" clubs
formed by young boys. They often consist of four to
nine beginning phreak/hackers who will assist each
other in obtaining telephone credit-card numbers. By
pooling their resources, a large number of illicit
"codez" can be obtained and shared with others.
Distribution of the account numbers is not limited to
the group, they are often shared with the community at
large, "courtesy of Codez Kidz Ltd." Groups of this
type are looked at with disdain by "elite"
phreak/hackers and are often criticized as being more
interested in self-promotion then they are with
actually phreaking or hacking.

Some hacker groups are very proficient and
dedicated to their craft, however. These groups are
characterized by smaller memberships, less visibility
to non-members, and commitment to the CU enterprise.
They are loosely organized, yet some have managed to
exist six or more years despite members dropping out or
being arrested. These "elite" groups are selective
about membership, and cite trust and talent as the two
leading requirements for joining:

> The group exists mainly for information
> trading. If you trust everyone else in the
> group, it is very profitable to pool

>information on systems . . . also it is nice
to know someone that you can call if you need
help on operating system X and to have people
feel free to call you if they need help on
operating system Y (AN, message log, 1988).

>Trust is a very important part of a group. I
think that's blatantly obvious. You have to
be able to trust the other members of the
group with the information you are providing
in order to be productive, and have a secure
situation (UU, message log, 1988).

>. . . all groups serve the same purpose: to
make their members feel better about
themselves (like, wow, I'm in a group) and to
trade things, whether it's wares, codes, or
whatever. But the thing is that being in a
group is like saying "I trust you, so like,
what can we do together?" (NN, message log,
1988)

Indeed, hacker groups are formed primarily for the

purpose of information exchange. To this end, groups

attempt to recruit members with a wide variety of

"specializations" in order to have a better support

network to turn to:

>%Our group% has always been very selective
about members (took me six years to get in).
The only reason the group exists is to bring
together a diverse group of talents. There is
very little overlap in %the group% these
days. Everyone has one thing that they are
the best in the country at, and are
conversant with just about any other form of
hacking. As an example, I got into a Primos
computer this morning around 9 am. Once I got
in, I know enough about Primos to get around,
but that's it. So I call %PS% in New York,
give him the info, and when I get home
tonight, he has gotten in and decrypted the
entire username/password file and uploaded it
to me. But two weeks ago he got into a VAX.
He got the account to me, I called it up and
set up three backdoors into the system that
we can get in if the account is detected or
deleted. Simple matter of communism. From
each according to his ability . . . etc. Also
it helps that everyone in the group is
experienced enough that they don't fuck up
accounts you spend all day getting (TM, field
notes, 1989).

Consistent with the Best and Luckenbill ideal

type, hacker groups do not exhibit a set division of

authority or labor. Most groups are leaderless, and

every member is free to pursue their own interests,

involving other members of the group only when desired:

>   We just got our group together. We've got a
>   guy that does VMB's and a Sprinter %obtains
>   "codez" from U.S. Sprint% and a couple of
>   hackers. Everybody's free to pursue whatever
>   system they want but if they want or need
>   some help they can call on any of the other
>   members if they want to. Like if one guy is
>   scanning and finds a VAX he might call and
>   give me the dialup. Then I might have to
>   call our Sprinter to get some codez so I can
>   start hacking on it. Once I get through I'll
>   give the account to the other members. But
>   if I found it myself I wouldn't have to give
>   it out but I probably would anyway 'cuz
>   keeping it would be bullshit (DC, field
>   notes, 1988).
>
>   There isn't a leader really. The guy who
>   starts the group sort of acts like a contact
>   point but everyone else has everyones' phone
>   number and you can call whoever you want to
>   anytime. Usually when you're putting a group
>   together you just get everyone you want and
>   you all decide on a name. (DC, field notes,
>   1988).

Summary

By virtue of the extensive social network found in the CU, some participants form work groups. The sophistication of these groups varies, but in all cases it is evident that the groups exist to support what are primarily individually performed activities. The groups exhibit many of the ideal-type characteristics of peer associations, and it is clear that in some cases the computer underground is socially organized as peers.

Conclusion

Phreakers, hackers, and pirates do not act as loners. Loners do not associate with others, and are on their own in coping with the practical problems presented by their activities (Best and Luckenbill 1982, p.28). From the data presented here, it is evident that the computer underground has established an extensive social network for the exchange of resources and mutual support. The characteristics of the CU varies according to the goals of the participants, but the presence of mutual association is

consistent. Contact between individuals is limited,
with the acts of phreaking or hacking being committed
alone. Computer underground participants do associate
with one another in order to discuss matters of common
interest, such as performance techniques, news, and
problem solving. To facilitate this informational
exchange, they have established a technologically
sophisticated network that utilizes computer bulletin
boards, voice mail boxes, telephone bridges, and
telephone loops.

        The collegial organization of the computer
underground is further evidenced by the establishment
of a CU culture. The subcultural adaptation of
language, expectations of normative conduct, and status
stratification based on mastery of cultural knowledge
and skill, all indicate that the computer underground
is, at the very least, a social organization of
colleagues (see Best and Luckenbill, 1982, p.37).

        The very structure that permits mutual association
among CU participants also encourages some to form
working relationships, thus acting as peers by mutually
participating in CU activities. Peers organized in this
manner share in their deviance, organizing informally
with little division of labor or set division of
authority (Best and Luckenbill, 1982, p.45). These
peer associations provide support to members, and can
provide socialization and recruitment functions for
newcomers. The establishment of work groups, through
mutual participation, indicates that though the
computer underground is largely organized as a network
of colleagues, it is also, to some degree, a social
organization of peers.

        Best and Luckenbill (1982) describe two additional
forms of deviant associations that are more

organizationally sophisticated than peers: "mobs" and
"formal organizations." The computer underground,
however, does not display the requisite characteristics
of these organizational types. The primary
characteristic of "mobs" is an elaborate division of
labor (Best and Luckenbill, 1982, p.25). While some CU
groups do exhibit a rudimentary division of labor based
on individual members' specialization, it is not by any
means "elaborate." Any division of labor that does
exist is voluntary and arises on the basis of
specialized knowledge, not a specialized organizational
role.

     In much the same manner the lack of a designated
leader or leadership hierarchy prevents CU groups from
being categorized as "formal organizations" in the Best
and Luckenbill typology. Deviant organizations at this
level are quite sophisticated and there is no empirical
evidence that the computer underground is organized in
this manner.

     This study of the computer underground has been a
test of the Best and Luckenbill typology of the social
organization of deviants. As a test of their
organizational indicators, the CU has shown that the
categories are well constructed, with the possible
exception of limiting "mutual participation" to acts
carried out in the presence of others. However, if we
modify this to include non-simultaneous, but
cooperative, acts as found in phreak/hacker groups, the
category is otherwise robust. The flexibility of the
typology, which explicitly recognizes that not all
deviant associations will display all of the character-
istics (Best and Luckenbill, 1982, p.25), is a strength
that allowed it to be easily used in terms of the
computer underground.

By addressing the CU from a social organizational
viewpoint we have seen that despite the high technology
trappings of their craft, pirates, phreakers, and
hackers display organizational characteristics found in
other groups that have been criminalized. This may
suggest that the development of sophisticated tools to
commit "crime" does not necessarily affect the ways in
which individuals organize their activities.

The implications of peer and collegial
organization for the members of the computer
underground are vast. The level of sophistication has
a direct relationship to the types of resources on
which individuals can draw (Best and Luckenbill, 1982,
p.54). Because CU members are mutually associated,
they are able to turn to colleagues for advice and
support with various problems. However, at the
collegial level they are left to enact the solutions
independently. Whether or not they are successful in
doing so will determine if they choose to remain active
in the computer underground. The data show that
involvement in the CU is short in duration, unless
success in early phreak/hack attempts is obtained. As
long as the CU remains organized as a collection of
colleagues, this trend will continue. Additionally, as
the computer and telephone industries become more
sophisticated in preventing the unauthorized use of
their facilities, new phreak/hackers are unlikely to
succeed in their initial attempts at the act, thus
dropping away from the activity and never becoming
acculturated to the point where peer relationships can
be developed.

At the peer level, a dimension of sophistication
that some members of the CU do display, the knowledge
and resources to solve problems and obtain resources is

greater. However, even at this level the ties between

peers remain weak at best. Although their cooperative

ties allow for more sophisticated operations, and

somewhat reduce the CU's vulnerability to social

control agents (Best and Luckenbill, 1982, p.53), it

still does not completely eliminate the need for

individual success in order to sustain a CU career. As

long as the CU remains at the current level of

organizational sophistication, with weak ties and

somewhat limited means of support and resource

attainment, it will continue to be a transitory and

limited "criminal" enterprise.

This realization should be considered by policy

makers who desire to further criminalize computer

underground activities. Given the current organization

of the CU, the future social costs of their actions are

not likely to expand beyond the current level. There

is no evidence to support assertions that the CU is

expanding, and the insight provided here shows that it

is not likely to do so on a large scale.

For sociologists, the computer underground is a

field rich for insight into several areas of concern.

Future research into the career path of CU members, and

the relationships between individuals, could prove

helpful to those interested in applying theories of

differential association and career deviance.

Additionally, the computer underground provides a

unique opportunity to study the process of

criminalization, and its effect on those who are

engaged in the behavior.

REFERENCES

Best, Joel and David F. Luckenbill. 1982. Organizing
Deviance. Englewood Cliff, New Jersey: Prentice-Hall.

Bequai, August. 1987. Technocrimes. Lexington,
Mass.:Lexington Books.

Bickford, Robert. 1988. Personal communication to Gordon Meyer.

Chicago Tribune. 1989. "Computer hacker, 18, gets prison for fraud." Feb. 15:2,1.

Field Notes. Interviews with phreakers, hackers, and pirates. Conducted from 7/88 to 4/89 (confidential material in authors files).

Hollinger, Richard C. and Lonn Lanza-Kaduce. 1988. "The Process of Criminalization: The Case of Computer Crime Laws." Criminology 26:101-126.

Levy, Steven. 1984. Hackers: Heroes of the Computer Revolution. New York: Dell Publishing.

Message Logs from a variety of computer underground bulletin board systems, (confidential material), 1988-1989.

NBC-TV. 1988. Hour Magazine. November 23, 1988.

Parker, Donn B. 1983. Fighting Computer Crime. New York: Charles Scribner's Sons.

Rosenbaum, Ron. 1971. "Secrets of the Little Blue Box." Esquire October, pp. 116-125.

Small, David. 1988. Personal communication to Gordon Meyer.

WGN-Radio. 1988. Ed Schwartz Show. September 27, 1988.

APPENDIX A
COMPUTER UNDERGROUND PSEUDONYMS

Literature, films, and Entertainment	Computers & related technology	Nouns, titles & Descriptive names
Pink Floyd	Mrs. Teletype	The Professor
Hatchet Molly	Baudy Bastard	Perfect Asshole
Jedi Knight	Doctor Phreak	The Messiah
King Richard	Lord FAX	Right Wing Fool
Captain Hoga	CNA Office	Bed Bug
Al Crowley	Sir Mac	Sleepy Head
Doc Holiday	Busy Signal	Mean Underwear
Mr. Big Dog	Silicon Student	Cockroach
Robin Williams	Fiber Cables	Primo Bomber
Big Bird	Phone Crasher	The Prisoner
Cross-eyed Mary	Doc Cryptic	Night Lighting
Capt. America	Apple Maniac	No Regrets
Uncle Sam	Fuzzy Sector	Grounded Zero
Thumpr	Cntrl. Alt. Del.	Spit Wad
Little John	Byte Ripper	Shadow Dove

APPENDIX B
NEW USER QUESTIONNAIRE FROM A PHREAK/HACK BBS

    Welcome to Analog Electronics Datum System. Please take this time to fill out a one-time questionnaire that will allow us to determine your level of access on Analog Electronics Datum System.

        If any question is too difficult for you to
answer, just answer with your best guess or a simple "I
don't know."

        We basically have two different divisions or types
of users on this system:

                (1) Apple (%%,Mac), and IBM software traders
                (2) Telecommunication hobbyists - any/all
                    computers (networks, mainframes,
                    engineering)

        Your answers will help us decide which category
you belong to and what access you should get on our
system.

* What type of computer & modem are you using to call
this system?

* Where did you get the phone number to Analog
Electronics Datum System?

* We'll need your first name and real phone # where you
can be reached for validation purposes only, this
information is kept in a password encoded file, on
another computer (critical for higher validation):

First for the FILE TRANSFER AREA ACCESS questions:

(1) How many bits are in a nibble? (Assume 6502 micro
    processor)

(2) Define WORM, RAM, ROM, VDT, CRT, BPS? (Pick any 3)

(3) What does 2400 baud mean in terms of bit transfer
    speed?

(4) What is PT,MT,AE,BIN2,Ymodem Batch,BLU? (Pick any
    4)

(5) How many Megahertz does a standard Apple %%+ run
    at? (rounding OK)

Now for the TeleCommunication Questions:

(1) Describe the Voice Transmission Use of a Loop:

(2) If I gave you my phone #, how would you find my
    name and address?!

(3) Can you name any networking software operating
    systems or protocols?

(4) What is the highest frequency a twisted two wire
    pair can transmit at?

(5) We believe Phones and Computers Belong Together,
    what do you BELIEVE?

Ok, thanks for that info.

        A MESSAGE FROM AL CAPONE (LOCAL) AND THE TRADER (LD)
                        SYSTEM VALIDATORS

        Welcome to ALDS! As a new user you have made
a change for the better in choosing this system as
one of your places of telecommunication exchange.   In
my opinion, this is one, if not the best, system
in telecommunications today as most of the good boards
such as Shadowspawn, Metal Shop Private, etc. do not
exist anymore. Quality users exist on this system that
have established a reputation for themselves so
questions you ask will be answered thoroughly and
precisely. We are a sponsor board of the LOD/H
Technical Journal, and accounts have been
established representing Phrack, Inc. and 2600
Magazine. (For our software trading people, we also
have an excellent file transfer area . . . consistent
with the rest of the nation . . .)

        Due to the high quality of our system, we will
need some additional information about you.
Maintenance of a high quality system requires high
quality users, so the first step in this process is
keeping the low quality users off of the system . . .
so please cooperate with us . . . this is for your
benefit as well as ours.   The information you give us
will be cross referenced with other systems for
accuracy, and if you leave false information, you may
suffer low access or deletion.

        All phone number information is stored outside of
the housing of this system inside of an encrypted,
password locked file for your security. So if you have
left an invalid phone #, please leave one where you can
be reached, or someone's name and number (if possible)
that will vouch for you. Keep in mind this validation
can take up to 1 week to complete due to the high
volume of new callers to our system.

Note: Limited system access will be granted within 24
Hrs if all of your info seems correct.

Thanks in advance . . .   Bugsy Malone
                                   The Swapper
                                SYSOP/SYSTEM VALIDATORS

% Bugsy Malone needs the following info: %

(1) Your references (sysops, other users on this
    system, other BBS).
(2) Your interests in having access to our system.
(3) How do you feel you can contribute to our system?
(4) How many years of telecommunication experience do
    you have?
(5) Do you have any special talents in programming, or
    operating systems?
    If yes, then name the language(s) or operating
    system(s).

Enter message now, answering these questions:

%after entering the message the BBS hangs up and the
caller will call back in 24 hours to see if access has
been granted.